UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/698,498	10/30/2003	Sanjay Aiyagari	50325-0805	9591

29989 7590 07/25/2008

HICKMAN PALERMO TRUONG & BECKER, LLP
2055 GATEWAY PLACE
SUITE 550
SAN JOSE, CA 95110

EXAMINER
KIM, PAUL

ART UNIT	PAPER NUMBER
2161	

MAIL DATE	DELIVERY MODE
07/25/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/698,498	AIYAGARI ET AL.	
	Examiner	Art Unit	
	PAUL KIM	2161	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *23 April 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-4,6,7,9-16,18-20,39-42,44,45,47-51,53,54 and 56-58* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-4, 6-7, 9-16, 18-20, 39-42, 44-45, 47-51, 53-54, 56-58* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This Office action is responsive to the following communication: Amendment filed on 23 April 2008.

2. Claims 1-4, 6-7, 9-16, 18-20, 39-42, 44-45, 47-51, 53-54, 56-58 are pending and present for examination.

Response to Amendment

3. Claims 1, 9, 10, 18, 39, 47, 48, and 56 have been amended.

4. Claims 46 and 55 have been cancelled.

5. No claims have been added.

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. **Claim 1-4, 7-11, 13, 16-17, 18-20, 39-42, 45-49, 51 and 54-58** rejected under 35 U.S.C. 103(a) as being unpatentable over Indicula et al (U.S. Patent No. 6,950,822, hereinafter referred to as INDICULA), filed on 25 November 2002, and issued on 27 September 2005, in view of Deinhart et al (U.S. Patent No. 5,911,143, hereinafter referred to as DEINHART), filed on 14 August 1995, and issued on 8 June 1999, and in further view of Jensenworth et al (U.S. Patent No. 6,279,111, hereinafter referred to as JENSENWORTH), filed on 12 June 1998, and issued on 21 August 2001.

8. **As per claims 1, 10, 18, 39, 48 and 56,** INDICULA, in combination with DEINHART and JENSENTWORTH, discloses:

A method for controlling access to a resource of a plurality of resources, the method comprising the steps of:

creating and storing in a filesystem of an Operating System a plurality of files that each represents a different resource of the plurality of resources {See JENSENWORTH, C4:L42-50};

assigning an access value to a file attribute of a file that represents the resource, wherein the file attribute is used by the Operating System to manage file access, wherein the access value corresponds to a combination of a particular role and the resource {See JENSENWORTH, C5:L4-21, wherein this reads over "[t]he object 72 has a kernel level security descriptor 76 associated therewith, and the object manager 74 provides the security descriptor 76 and the token 60 to a security mechanism" and "[t]he contents of the security descriptor 76 are typically determined by the owner (e.g., creator) of the object, and generally comprise a (discretionary) access control list (ACL) 80 of access control entries, and for each entry, one or more access rights"};

receiving user-identifying information from a user requesting access to the resource, wherein the user-identifying information comprises a role associated with the user {See IDICULA, C5:L11-13, wherein this reads over "user information that indicates a user of the associated connection, the user's roles, and the user's privileges, among other information about the user"}, wherein the role is determined from a user identifier uniquely associated with the user and from a group identifier associated with a group that includes the user {See DEINHART, C1:L31-36, wherein this reads over "[i]n most of the installed computer systems access rights are granted or revoked explicitly for individual users or group of users on respective data or, more generally, on respective objects by a system administrator"};

receiving a resource identifier associated with the resource {See IDICULA, C7:L19-35, wherein this reads over "[i]f a session is already created for this client, a session object 122 associated with the client is indicated in the process state object 130"};

creating an access identifier based on the user-identifying information and the resource identifier, wherein the access identifier is formatted as a file attribute that is used by the Operating System to manage file access {See IDICULA, C4:L42-56, wherein this reads over "session objects 122, one or more process state objects 130a, 130b, collectively referenced hereinafter as process state objects 130, and a session pool object 140. In object-oriented technologies, an object is a data structure that stores data that indicates one or more attributes or methods or both"};

calling the Operating System to perform a file operation on the file, wherein calling the Operating System includes providing the access identifier to the Operation System {See IDICULA, C1:L52-62, wherein this reads over "[a] session is a related series of one or more requests for services made over a communication channel. The channel is typically established by the operating system of the host for the database server"; and C7:L19-30, wherein this reads over "[i]f a session is already created for this client, a session object 122 associate with the client is indicated in the process state object 130; and that session object 122 is used"}; and

granting the user access to the resource when the Operating System call successfully performs the file operation {See IDICULA, C7:L20-21, wherein this reads over "a request is received from database client 102a for database services"}, wherein the Operating System call successfully performs the file operation if the access identifier matches the access value {See JENSENWORTH, C5:L15-21, wherein this reads over "[t]he security mechanism

78 compares the security IDs in the token 60 along with the type of action or actions requested by the process 70 against the entries in the ACL 80. If a match is found with an allowed user or group, and the type of access desired is allowable for the user or group, a handle to the object 72 is returned to the process 70"};

wherein the file operation on the file representing the resource is selected from a group consisting of opening the file, closing the file, deleting the file, reading from the file, writing to the file, executing the file, appending to the file, reading a file attribute, and writing a file attribute {See IDICULA, C7:L19-30, wherein this reads over "[i]f a session is already created for this client, a session object 122 associate with the client is indicated in the process state object 130; and that session object 122 is used"}.

While INDICULA fails to expressly disclose the determination of a role "from a user identifier uniquely associated with the user and from a group identifier associated with a group that includes the user," DEINHART discloses the grant or revocation of access rights for "individual users or group of users . . . on respective objects." Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the above invention suggested by INDICULA by combining it with the invention disclosed by DEINHART.

Additionally, while INDICULA may fail to expressly disclose the method steps of assigning an access value to a fire attribute of a file and the Operating System call successfully performs the file operation if the access identifier matches the access value, JENSENWORTH discloses a security model using restricted tokens for file and resource access. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the above invention suggested by INDICULA by combining it with the invention disclosed by JENSENWORTH.

One of ordinary skill in the art would have been motivated to do this modification so that where a user falls within a classified group of users (e.g. System Administrator or Guest), a user identifier may be associated with the user accordingly.

9. **As per dependent claims 2, 11, 19, 40, 49 and 57**, it would be inherent for the role identifier and resource identifier to be stored in a first and second set of bits, respectively, since files are comprised of a sequence of bits.

10. **As per dependent claims 3, 20, 41 and 58**, INDICULA, in combination with DEINHART and JENSENTWORTH, discloses:

A method as recited in Claim 1, wherein:

the step of creating an access identifier based on the user-identifying information and the resource identifier comprises formatting the access identifier as a group identifier file attribute {See DEINHART, C1:L31-36, wherein this reads over "[i]n most of the installed computer systems access rights are granted or revoked explicitly for individual users or group of users on respective data or, more generally, on respective objects by a system administrator"}; and

the step of calling the Operating System to perform an operation on the file representing the resource comprises:

assigning the access identifier to a group identifier attribute of an Operating System process {See IDICULA, C4:L42-56, wherein this reads over "session objects 122, one or more process state objects 130a, 130b, collectively referenced hereinafter as process state objects 130, and a session pool object 140. In object-oriented technologies, an object is a data structure that stores data that indicates one or more attributes or methods or both"}; and

calling an Operating System routine from the Operating System process to perform the operation on the file representing the resource {See IDICULA, C1:L52-62, wherein this reads over "[a] session is a related series of one or more requests for services made over a communication channel. The channel is typically established by the operating system of the host for the database server"; and C7:L19-30, wherein this reads over "[i]f a session is already created for this client, a session object 122 associate with the client is indicated in the process state object 130; and that session object 122 is used"}.

11. **As per dependent claims 4, 13, 42 and 51**, INDICULA, in combination with DEINHART and JENSENTWORTH, discloses:

A method as recited in Claim 1,

wherein the step of calling the Operating System to perform an operation on the file representing the resource comprises comparing the access identifier to an identifier included in an Access Control List file attribute associated with the file representing the resource {See DEINHART, C1:L31-41, wherein this reads over "[w]hen an access request occurs during operation time of the computer system from a user or, more generally, from a subject to the object, then the security system looks at the access control list of the respective object and decides whether the subject may access the object in the request manner"},

wherein the Access Control List file attribute includes the identifiers of all users and all groups of users allowed to access the file representing the resource {See DEINHART, C1:L31-36, wherein this reads over "[i]n most of the installed computer systems access rights are granted or revoked explicitly for individual users or group of users on respective data or, more generally, on respective objects by a system administrator"}.

12. **As per dependent claims 7, 16, 45 and 54**, the claim does not carry patentable weight since the claim recites the file operation of "opening the file representing the resource," which was optionally recited in claims 1, 10, 18, 22, 31, 39, 48 and 56 (i.e. "wherein the file operation on the file representing the resource is selected from a group consisting of opening the file, closing the file, deleting the file,

reading from the file, writing to the file, executing the file, appending to the file, reading a file attribute, and writing a file attribute"), upon which the said respective claims depend. Therefore, since the opening of the file is optional and not necessary to the claimed invention, the claim is rejected.

13. **As per dependent claims 8, 17, 46 and 55**, INDICULA, in combination with DEINHART and JENSENTWORTH, discloses:

> A method as recited in Claim 1, wherein the step of representing the resource by a file stored in the Operating System filesystem comprises:
>
> creating the file representing the resource in the Operating System filesystem {See IDICULA, C4:L42-56, wherein this reads over "session objects 122, one or more process state objects 130a, 130b, collectively referenced hereinafter as process state objects 130, and a session pool object 140. In object-oriented technologies, an object is a data structure that stores data that indicates one or more attributes or methods or both"}; and
>
> assigning an access value to a file attribute of the file representing the resource, the file attribute being used by the Operating System to manage file access {See IDICULA, C4:L42-56, wherein this reads over "session objects 122, one or more process state objects 130a, 130b, collectively referenced hereinafter as process state objects 130, and a session pool object 140. In object-oriented technologies, an object is a data structure that stores data that indicates one or more attributes or methods or both"}, wherein the access value corresponds to a combination of a role {See IDICULA, C5:L11-13, wherein this reads over "user information that indicates a user of the associated connection, the user's roles, and the user's privileges, among other information about the user"} and a resource {See IDICULA, C7:L19-35, wherein this reads over "[i]f a session is already created for this client, a session object 122 associated with the client is indicated in the process state object 130"}.

14. **As per dependent claims 9 and 47**, INDICULA, in combination with DEINHART and JENSENTWORTH, discloses:

> A method as recited in Claim 8, wherein the file attribute used by the Operating System to manage file access is a group identifier file attribute {See DEINHART, C1:L31-36, wherein this reads over "[i]n most of the installed computer systems access rights are granted or revoked explicitly for individual users or group of users on respective data or, more generally, on respective objects by a system administrator"}.

15. **Claims 6, 12, 15, 44, 50 and 53** are rejected under 35 U.S.C. 103(a) as being unpatentable over Indicula et al, in view of Deinhart et al and Jensenworth et al, and in further view of Lewis (U.S. Patent No. 6,233,576, hereinafter referred to as LEWIS), filed on 25 September 1995, and issued on 15 May 2001.

16. **As per dependent claims 6, 15, 44 and 53**, INDICULA, in combination with DEINHART, JENSENWORTH, and LEWIS, discloses:

A method as recited in Claim 1, the method further comprising the steps of:

reading a permission bit associated with the file representing the resource, wherein the permission bit corresponds to the operation performable on the file representing the resource {See LEWIS, C14:L6-12, wherein this reads over "derive the authorization file names and the permission bits (from the resource class and name), and to apply the appropriate permissions"};

based on the operation on the file indicated by the permission bit, determining a resource operation that is performable on the resource {See LEWIS, C16:L64-C17:L4, wherein this reads over "[t]he resulting access rights consist of a three bit filed with the following meanings . . ."}; and

granting the user the privilege of performing the resource operation on the resource {See DEINHART, C1:L31-41, wherein this reads over "[w]hen an access request occurs during operation time of the computer system from a user or, more generally, from a subject to the object, then the security system looks at the access control list of the respective object and decides whether the subject may access the object in the request manner"} only if the permission bit allows the operation to be performed on the file representing the resource {See LEWIS, C17:L5-9}.

While INDICULA and DEINHART fail to expressly disclose the use of permission bits in determining user privileges, LEWIS discloses the use of permission bits which signify Read, Write, or Execute authority. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the above invention suggested by INDICULA and DEINHART by combining it with the invention disclosed by LEWIS.

One of ordinary skill in the art would have been motivated to do this modification so that files may contain permission bits which allow users the permission to certain operations on the file.

17. **Claims 6, 12, 15, 44, 50 and 53** are rejected under 35 U.S.C. 103(a) as being unpatentable over Indicula et al, in view of Deinhart et al and Jensenworth et al, and in further view of Official Notice.

18. **As per dependent claims 12 and 50**, INDICULA, in combination with DEINHART, JENSENWORTH, and Official Notice, discloses:

A method as recited in Claim 10, wherein the step of making an Operating System call to perform an operation on the file representing the resource comprises:

storing the group identifier value of a group identifier attribute of an Operating System process {See DEINHART, C1:L31-36, wherein this reads over "[i]n most of the installed computer systems access rights are granted or revoked explicitly for individual users or group of users on respective data or, more generally, on respective objects by a system administrator"};

assigning the access identifier to the group identifier attribute of the Operating System process {See IDICULA, C4:L42-56, wherein this reads over "session objects 122, one or more process state objects 130a, 130b, collectively referenced hereinafter as process state objects 130, and a session pool object 140. In object-oriented technologies, an object is a data structure that stores data that indicates one or more attributes or methods or both"};

calling an Operating System routine from the Operating System process to perform the operation on the file representing the resource {See IDICULA, C1:L52-62, wherein this reads over "[a] session is a related series of one or more requests for services made over a communication channel. The channel is typically established by the operating system of the host for the database server"; and C7:L19-30, wherein this reads over "[i]f a session is already created for this client, a session object 122 associate with the client is indicated in the process state object 130; and that session object 122 is used"}, wherein the operation on the file representing the resource is performed only if the value of the group identifier attribute of the Operating System process matches the value of the group identifier file attribute of the file representing the resource {See IDICULA, C7:L20-21, wherein this reads over "a request is received from database client 102a for database services"}; and

resetting the group identifier attribute of the Operating System process to the stored group identifier value {See Official Notice}.

The Examiner takes Official Notice that it would have been obvious to one of ordinary skill in the art at the time the invention was made to reset the group identifier attribute of the Operating System process to the stored group identifier value. That is, where a group identifier is set, it would have been obvious to one of ordinary skill in the art to have the capability to reset said group identifier attribute accordingly.

Response to Arguments

19. Applicant's arguments with respect to claim rejections under 35 U.S.C. 103 have been considered but are moot in view of the new ground(s) of rejection.

Conclusion

20. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date

of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

21. Any inquiry concerning this communication or earlier communications from the examiner should be directed to PAUL KIM whose telephone number is (571)272-2737. The examiner can normally be reached on M-F, 9am - 5pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Apu Mofiz can be reached on (571) 272-4080. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Paul Kim
Examiner, Art Unit 2161
TECH Center 2100

/pk/

/Apu M Mofiz/
Supervisory Patent Examiner, Art Unit 2161